一般社団法人 電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report

ビットコイン利用者の特定・追跡の仕組みに関する考察

才所 敏明[*1] 辻井 重男[*2] 櫻井 幸一[*3]

*1 (株)IT 企画 〒158-0083 東京都世田谷区奥沢 6-18-10
*2 中央大学研究開発機構 〒112-8551 東京都文京区春日 1-13-27
*3 九州大学大学院システム情報科学研究院 〒819-0395 福岡市西区元岡 744 番地,
(株) 国際電気通信基盤技術研究所 〒619-0288 京都府相楽郡精華町光台二丁目 2 番地 2
E-mail: *1 toshiaki.saisho@advanced-it.co.jp, *2 tsujii@tamacc.chuo-u.ac.jp, *3 sakurai@INF.kyushu-u.ac.jp

あらまし 暗号資産の強い匿名性によるマネーロンダリングや不正・不法な取引の決済への利用が急増しつつあり, 暗号資産の悪用を防ぐ対策が求められている. 各国の政府は暗号資産関連事業者に対し確実な KYC(本人確認)を実施する等, 法制度やガイドラインにより規制を強化している. しかし, 多くの暗号資産は事業者を通さず利用者間での資産移転が可能なため, このような対策の効果は限定的であり, 暗号資産の悪用を防ぐには, 暗号資産システム側で利用者の特定・追跡のための仕組みを組み込む必要がある. 本論文では, ビットコインシステムの資産移転方式 P2PKH を対象に, 利用者であるトランザクション作成者の特定・追跡方式についての考察結果を報告する.

キーワード 暗号資産, 匿名性, 特定・追跡性, 悪用対策, KYC, KYT, ビットコイン, P2PKH

Consideration on the mechanism of identifying and tracking Bitcoin users

Toshiaki Saisho[*1] Shigeo Tsujii[*2] Kouichi Sakurai[*3]

*1 Advanced IT Corporation 6-18-10 Okusawa, Setagaya-ku, Tokyo, 158-0083 Japan
*2 Research and Development Initiative, Chuo University 1-13-27 Kasuga, Bunkyo-ku, Tokyo, 112-8551 Japan
*3 Advanced Telecommunications Research Institute International 2-2-2 Hikaridai, Seika-cho, Souraku-gun, Kyoto, 619-0288 Japan
E-mail: *1 toshiaki.saisho@advanced-it.co.jp, *2 tsujii@tamacc.chuo-u.ac.jp, *3 sakurai@INF.kyushu-u.ac.jp

Abstract Due to strong anonymity of CryptoAssets, the use for money laundering and settlement of fraudulent and illegal transactions is increasing rapidly, and measures to prevent misuse of CryptoAssets are required. The governments of each country are tightening regulations through legal systems and guidelines, such as implementing reliable KYC (identity verification) for CryptoAssets business organizations. However, since many CryptoAssets can be transferred between users without going through CryptoAssets business organization, the effect of such measures will be limited. We think that, for preventing the misuse of CryptoAssets, it is necessary to incorporate a mechanism for identifying and tracking users in the CryptoAssets system. In this paper, we consider the method of identifying and tracking the transaction creator (CryptoAssets system user), targeting the asset transfer method P2PKH of the Bitcoin system.

Keywords CryptoAssets, Anonymity, Identifiability/Trackability, Abuse, KYC, KYT, Bitcoin, P2PKH

1. はじめに

ビットコインをはじめとする多くの暗号資産は一定レベルの匿名性が確保されているが, プライバシーや個人情報の確実な保護の観点からは不十分であり, 暗号資産の匿名性を強化する研究開発が展開され, 実際に匿名性が強化された暗号資産も提案されている ([1], [2]).

一方, 暗号資産の匿名性は, マネーロンダリングや不正・不法な取引の決済手段としての利用を急増させる原因ともなっており, 大きな社会問題となっている. このような暗号資産の悪用を防止・抑止するためには, 暗号資産の利用者の確実な特定・追跡性が必要であるが, そのための技術・仕組みの検討は未だ緒に就いたばかりの状況である.

一般に, 匿名性と特定・追跡性は対立する概念ではあるが, 安心・安全な社会の実現には, その両立が必要である. 匿名性の強い暗号資産システムにおいても, 特定・追跡性の仕組みの導入が期待されている.

本論文では, 資産移転情報を台帳に登録・管理する資産移転記録方式 ([3]) の暗号資産 (TCAMS : Transaction based CryptoAssets Management System) で

あるビットコインを対象にした，トランザクション作成者（利用者）の特定・追跡の仕組みの検討結果を報告する．

2. ビットコインシステム

資産（ビットコイン）の移転を示すトランザクションはワレットで生成され，ビットコインネットワークで承認されブロックチェーンに登録される．図１にビットコインシステムの構成およびトランザクションの流れを示している．

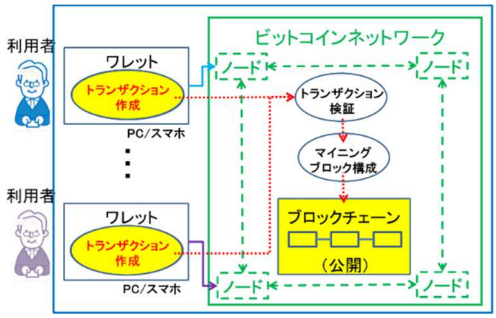

図１　ビットコインシステム構成概要

本章では，ビットコインの利用者の特定・追跡を困難とする要因である，ビットコインブロックチェーンに登録され公開されるトランザクションが利用者の一定レベルの匿名性を確保していること，を示す．

2.1. トランザクション/ワレット

トランザクションは利用者（トランザクション作成者)のワレットで作成される.トランザクションでは，利用者（提供者）が保有するビットコインを他の利用者（受取者）へ提供する，資産移転情報が指定されている．受取者の指定には様々の方法がビットコインで用意されているが，本論文では標準的な指定方法である P2PKH（Pay to Public Key Hash）を対象に検討することとする．P2PKH を利用したトランザクションに含まれる利用者（提供者および受取者）に関する情報を図２に示している．

図２トランザクション内の資産移転情報（P2PKH）

トランザクションに含まれる利用者に関する情報①～④の詳細は以下の通り．

① 提供者が使用する入力資産の指定

提供者は使用する資産として，自身が過去に受け取った資産（提供者が受取者として指定されている出力資産）であり未使用である資産へのポインタを指定する．指定された出力資産では，今回の提供者の公開鍵のハッシュ値および金額の２つの情報が指定されている．

提供者の公開鍵は，ビットコインでは乱数から生成される都度異なる公開鍵の利用が推奨されており，提供者の公開鍵のハッシュ値から利用者の特定・追跡は難しい．また，金額（提供額）にも，利用者の情報が直接は含まれておらず，利用者の特定・追跡は難しい．

以上のように,「提供者が使用する入力資産の指定」の情報は，利用者の一定レベルの匿名性を確保している．

②提供者が使用する入力資産の所有権の証明

提供する資産の所有権の証明として，提供者が受取時に指定した公開鍵のハッシュ値に対応する公開鍵そのもの，およびその公開鍵に対応する秘密鍵によるトランザクションへの署名を指定する．

指定する公開鍵は，既述の通り，提供者が必要の都度，乱数より生成するため，その公開鍵から利用者の特定・追跡は難しい．また，トランザクションへの署名から，使用した秘密鍵の導出，その秘密鍵に対応する公開鍵の導出は難しく，更には提供者が必要の都度異なる鍵ペアを乱数により生成するため，提供者の特定・追跡は難しい．

以上のように,「提供者が使用する入力資産の所有権の証明」の情報は，利用者の一定レベルの匿名性を確保している．

③受取者の指定

提供者は受取者が指定した公開鍵のハッシュ値を受取者として指定する．そのために，受取者は受取の都度,乱数を使用し新たな鍵ペアを生成し，生成された公開鍵のハッシュ値を提供者へ通知する．既述の通り，受取者の公開鍵のハッシュ値から受取者（利用者）の特定・追跡は難しく,「受取者の指定」の情報は，利用者の一定レベルの匿名性を確保している．

④受取額の指定

既述の通り，金額（受取額）には，利用者の情報が直接は含まれておらず，利用者の特定・追跡は難しく,「受取額の指定」の情報は，利用者の一定レベルの匿名性を確保している．

以上のように，ワレットで作成されるトランザクションに含まれる利用者に関する情報は，利用者の一定レベルの匿名性が確保されており，その情報から利用者を特定・追跡するのは難しい．

2.2. ブロックチェーン/ビットコインネットワーク

ワレットで生成されたトランザクションは，ビット

コインネットワークを構成する一つのノードへ送信される．受信したノードは別のノードへトランザクションを転送，その繰り返しにより，トランザクションはビットコインネットワーク全般に広く伝搬される．また，ノードではトランザクションの内容が適切かどうかの検証処理が実施され，その後，検証済みの多数のトランザクションにより構成されるブロックのマイニング競争が実施され，承認されたブロックがブロックチェーンに登録される（図３）．このような，ワレットで作成されたトランザクションがブロックチェーンに登録されるまでに実施されるトランザクションの内容にかかわる処理は検証処理のみである．

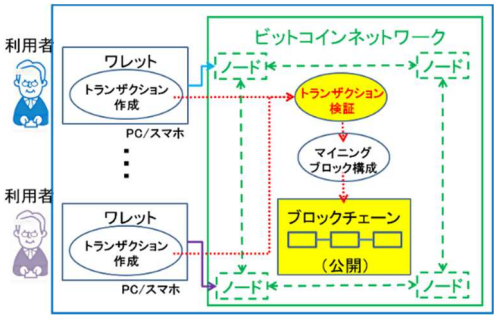

図３　ビットコインネットワークにおける トランザクション検証

検証処理で実施されるトランザクションの検証項目の中で，利用者に関する情報に対する主要な検証処理の内容および匿名性に対する影響は以下の通りである．

①入力資産の存在の確認

入力資産に指定された使用する資産の位置に出力資産が存在し，入力資産に指定された公開鍵と出力資産に指定されている公開鍵のハッシュ値が対応していることの確認であり，利用者の匿名性への影響は無い．

②入力資産の所有権を有することの確認

入力資産に指定された署名の公開鍵による検証による確認であり，匿名性への影響は無い．

③入力資産が未使用であることの確認

入力資産に指定された出力資産内の，受取者の公開鍵のハッシュ値が既に他のトランザクションの入力資産として指定されていないことの確認であり，匿名性への影響は無い．

以上のように，ワレットで作成された匿名性の強いトランザクションは，匿名性をそのまま維持しブロックチェーンに登録されるため，公開されるブロックチェーン上のトランザクション情報から利用者を特定・追跡することは難しい．

3. 不正・不法な暗号資産利用への対応状況

ビットコインをはじめとする暗号資産の匿名性は，利用者の個人情報・プライバシー情報の保護の観点からは重要な特性ではあるが，その匿名性を悪用した，不正・不法な取引の決済への利用やマネーロンダリング等が急増している．社会の安心・安全の維持のためには，このような暗号資産の悪用を検出・対処できる仕組みが不可欠である．ところが，前章で述べたように，現在のビットコインシステムではトランザクションの一定レベルの匿名性を確保しているが，利用者の特定・追跡性については考慮されていない．その他の暗号資産も同様の状況である．

そこで，各国は法制度により，ビットコインをはじめとする暗号資産の悪用の防止，検出，当該利用者への対応の仕組みを整備しつつある．具体的には，各国では暗号資産交換事業者に対し KYC（利用者の本人確認）を求め，不正・不法な取引の決済やマネーロンダリング等の実施者を容易に特定・追跡できる仕組みを目指している．日本でも，2016 年の犯罪収益移転防止法（犯収法)の改正により，暗号資産交換業者に対し KYC が義務化され，2020 年の改正により，本人確認の方法が厳格化されている．

しかし，各国の暗号資産交換事業者で実施されている現状の KYC は必ずしも確実な本人確認ではなく，2020 年時点でも世界の暗号資産交換事業者の半数以上が脆弱な KYC（本人確認）システムになっている，と報告されている([6])．日本も同様である．

更に，一般に暗号資産の取引は P2P で実施され，暗号資産交換事業者は関与しない．キャッシュアウト（暗号資産を法定通貨へ変換）の際には暗号資産交換事業者を経由することになるが，暗号資産交換事業者における確実な KYC だけでは暗号資産の不正・不法な取引の決済への利用やマネーロンダリング等の防止・抑止効果は限定的である．

一方，1989 年にマネーロンダリング・テロ資金対策等に取り組む主要国政府による枠組みとして OECD に事務局を設置し発足した金融活動作業部会（FATF：Financial Action Task Force）では，2019 年に暗号資産関連企業向けのガイドライン「トラベルルール」([7])を導入し利用者の確実な本人確認と特定・追跡のための情報取得・管理を求めている．取得・管理すべき具体的な情報項目は以下の通り．

（i）暗号資産の提供者の名前

（ii）暗号資産の提供者のアカウント番号（ワレット ID 等）

（iii）暗号資産の提供者の物理的（地理的）住所，国民識別番号，または暗号資産関連企業に対して提供者を一意に識別する顧客識別番号，または提供

者の生年月日と出生地
(iv) 受取者の名前
(v) 暗号資産の受取者のアカウント番号(ワレット ID 等)

本ガイドラインの順守に向けて，各国の政府は法制度の整備，暗号資産関連企業は管理・運用面での対応の検討を進めているようであるが，まだまだ緒に就いたばかりで，その完全順守の見通しは立っていない．

既述の通り，そもそも，現在の多くの暗号資産システムが，暗号資産関連企業の関与無しに，個人間で取引が可能なため，暗号資産関連企業への運用・管理面での法制度による規制だけでは，不正・不法な暗号資産利用への対応は難しく，暗号資産システム側の技術面の対応，管理・運用面の対応，それらを支える法制度面の対応の連携が必要であろう．

4. ビットコイン利用者の特定・追跡方式の検討

暗号資産システム側で必要な利用者の特定・追跡のための機能の調査のため，ビットコインシステムを対象とした利用者の特定・追跡の仕組みを検討した．以下，具体的に検討した P2PKH トランザクション作成者（利用者）の特定・追跡のための複数の仕組みを示し，それぞれの仕組みを比較している．

4.1. ビットコインネットワークのノード活用方式(A)

トランザクション作成者の特定・追跡のために必要な機能を，ビットコインネットワークを構成するノードで実装する方式である（図４）．

利用者はワレット経由でノードの一つへアクセス，確実な身元確認の上，本人確認情報（身元情報と当人確認情報等）を登録する．ノードは登録利用者には固有の ID を発行し，その利用者の本人確認情報を ID と共にローカルな DB へ登録し，管理する．

利用者が，トランザクションにより資産移転を行う際は，登録済みのノードへそのノードの識別子をトランザクション内に明記し登録済みの利用者の ID と共に送信する．受信したノードは，ID に対応する当人確認情報を使用し，ワレット経由，利用者の当人確認を実施し，成功した場合は次にトランザクション内容の検証を行い，その上でトランザクション ID（トランザクションのハッシュ値）をその利用者 ID と共に記録すると共に他のノードへ転送し，ビットコインネットワークへ広く伝搬する．

調査・捜査機関が疑わしいトランザクションの作成者を特定・追跡する場合，調査・捜査機関はビットコインシステム内の調査・捜査ノードへ依頼し、ブロックチェーン上の該当するトランザクションから「疑わしいトランザクションの作成者が使用したノード」を特定し,そのノードが管理する情報から作成者を特定、作成者の身元情報を入手することにより，作成者（利用者）を特定・追跡可能となる．

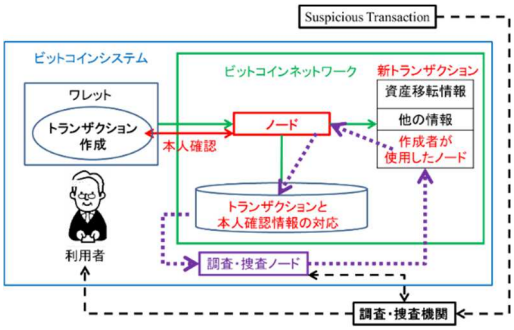

図４　ビットコインネットワークのノード活用方式（A）

4.2. 本人確認ノード導入方式(B)

トランザクション作成者の特定・追跡のために必要な機能を，新たに導入する本人確認ノードおよびブロックチェーンネットワークのノードで実装する方式である（図５）．

利用者の本人確認は本人確認ノードが担当し，本人確認に成功した場合は，利用者の ID および本人確認結果（公開鍵証明書）をワレットに発行し，同時に本人確認ノードにて登録・管理する．

利用者がトランザクションにより資産を移転させる場合は，本人確認結果の証明書と署名を付与しトランザクションを一つのノードへ送信する．受信したノードは証明書および署名を検証し，更にトランザクション内容の検証を行い，その上で証明書とトランザクション ID の対を登録しノード間で共有すると共に他のノードへ送信し，ビットコインネットワークへ広く伝搬する．

調査・捜査機関が疑わしいトランザクションの作成者を特定・追跡する場合，調査・捜査機関はビットコインシステム内の調査・捜査ノードへ依頼し、ノードで共有されている情報からトランザクションを作成した利用者の ID を特定し，その ID を使用し本人確認ノードが管理する情報から身元情報を入手することにより，作成者（利用者）を特定・追跡可能となる．

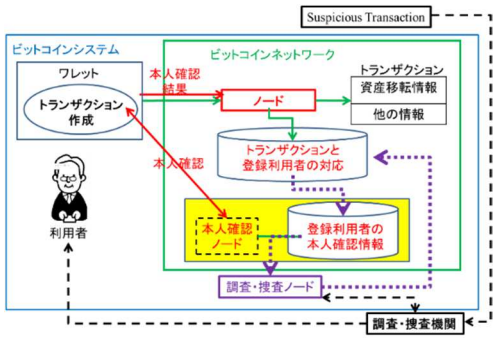

図５　本人確認ノード導入方式（B）

4.3. 本人確認ノード経由方式(C)

トランザクション作成者の特定・追跡のために必要な機能を，本人確認ノードで実装，ワレットは本人確認ノード経由，トランザクションをブロックチェーンネットワークのノードへ送信する方式である（図６）．

本人確認およびトランザクションと作成した利用者の対応の情報は本人確認ノードで実施する．本人確認情報および利用者とトランザクションの対応情報も本人確認ノードで記録・管理する．その上で，本人確認ノードの署名付きトランザクションをノードへ送信する．

受信したノードは本人確認ノードの署名検証の上，トランザクション内容の検証等の処理を行うと共に他のノードへ本人確認ノードの署名付きトランザクションを送信し，ビットコインネットワークへ広く伝搬する．なお，本人確認ノードの署名は，トランザクション検証後にマイニングプールへ登録される際に取り除かれ，ブロックチェーン上のトランザクション情報は従来通りとなることを想定している．

調査・捜査機関が疑わしいトランザクションの作成者を特定・追跡する場合，調査・捜査機関はビットコインシステム内の調査・捜査ノードへ依頼し、本人確認ノードが管理する情報から作成者の身元情報を入手することにより，作成者（利用者）を特定・追跡可能となる．

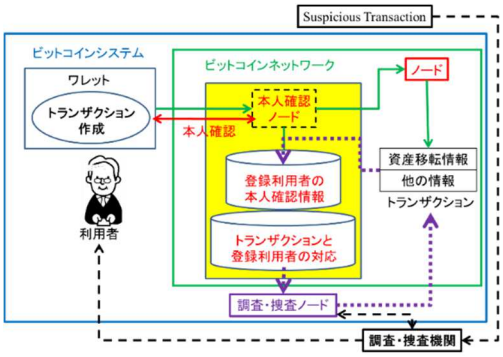

図６　本人確認ノード経由方式（C）

4.4. 本人確認基盤利用方式(D)

トランザクション作成者の特定・追跡のために必要な機能を，本人確認基盤 National Authentication Framework（[4]，[5]）および本人確認ノードで実装する方式である（図７）．

本人確認基盤は，筆者らが提案しているインターネットアプリケーションに共通に必要な本人確認を実施するフレームワークである.本人確認に成功した場合，利用者の ID および本人確認結果（公開鍵証明書）をワレットに発行し，同時に本人確認基盤にて登録・管理する．

利用者がトランザクションにより資産を移転させる場合は，本人確認結果の証明書と署名を付与しトランザクションを本人確認ノードへ送信する．本人確認ノードは証明書および署名を検証の上，証明書とトランザクション ID の対を登録する．その上で，本人確認ノードの署名付きトランザクションをノードへ送信する．

受信したノードは本人確認ノードの署名検証の上，トランザクション内容の検証等の処理を行うと共に他のノードへ本人確認ノードの署名付きトランザクションを送信し，ビットコインネットワークへ広く伝搬する．なお，本人確認ノードの署名は，トランザクション検証後にマイニングプールへ登録される際に取り除かれ，ブロックチェーン上のトランザクション情報は従来通りとなることを想定している．

調査・捜査機関が疑わしいトランザクションの作成者を特定・追跡する場合，調査・捜査機関はビットコインチェーンシステム内の調査･捜査ノードへ依頼し、本人確認ノード管理している情報からトランザクションを作成した利用者の ID を特定し，その ID を使用し本人確認基盤が管理する情報から身元情報を入手することにより，作成者（利用者）を特定・追跡可能となる．

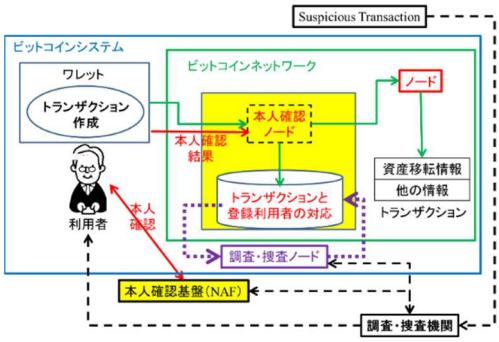

図７　本人確認基盤利用方式（D）

4.5. 各方式の比較

ビットコイン利用者の特定・追跡を可能とする仕組みの４つの実現方式を，次の５つの項目について評価する．

(1)既存のビットコインシステムへの影響の小ささ

社会実装のハードルを下げるため，現在のビットコインシステムの運用，管理を担当するシステム（ノードやワレット等）や組織の役割・責任への変更を極力少ない方式が望ましい．

(2) 利用者の個人情報・プライバシー情報の安全な管理のしやすさ

利用者の特定・追跡のためには，確実な本人確認が不可欠であるが，そのために保存すべき，身元情報,当人確認情報の収集･保存が必要である．身元情報，本人確認情報は，個人情報，プライバシー情報でもあり，その確実な保護が容易な方式

が望ましい.

(3) グローバルな暗号資産システム実現のしやすさ

利用者の本人確認の中の，特に身元確認は，各国の法制度強く依存している．多くの国の異なる身元確認方式，各国の関連組織と連携しながらの身元確認･当人確認を行いやすい方式が望ましい.

(4) 複数の暗号資産システムの利用のしやすさ

暗号資産利用者は複数の暗号資産を利用する．利用者にとって複数の暗号資産を使いやすい環境を実現可能な方式が望ましい.

(5) 早い実現時期が期待されるかどうか

(1)の評価項目とも関連するが，必要な仕組みのビットコインシステムでの早期実現の見通し，期待されるインターネット社会の基盤システムの早期実現の見通しのある方式が望ましい.

以上の評価項目について，実装方式の詳細は未定ではあるが，提案した 4 つの方式の可能性を 3 段階で評価した結果を図８に示している．本結果から，早期にビットコインシステムへの利用者の特定・追跡の仕組みを実装する場合は，方式（C）を選定し，本人確認基盤（NAF）が整備された段階で，方式（D）へ移行するのが，現実的アプローチと考えられる.

方式 / 評価項目	A	B	C	D
マイニング以降の処理への影響の小ささ	△	○	○	○
利用者の個人情報･プライバシー情報の安全な管理のしやすさ	×	△	△	○
グローバルな暗号資産システムの運用のしやすさ	×	×	△	○
複数の暗号資産システムの利用のしやすさ	×	△	△	○
社会実装の容易さ	×	×	○	△

図８　各方式の比較

5. おわりに

暗号資産の活用は増大し，それに伴って不正・不法な取引の決済やマネーロンダリング等での利用(悪用)も急増している.会の安心･安全を維持するためには，このような暗号資産の悪用の防止・抑止が可能な効果的対策が求められている.

各国政府では，暗号資産システムの運用にかかわる事業者への法制度やガイドラインによる規制・ルールの整備・強化等の対策が進められているが，事業者を経由せずに資産移転が可能な暗号資産システムでは効果は限定的で，暗号資産の移転を実施する暗号資産システム側の対応が必要であろう．暗号資産の不正・不法な取引の決済やマネーロンダリング等での利用（悪用）の防止・抑止には，暗号資産システム側の技術面の対応が必要であり，それを踏まえての管理・運用面の対応，それらを支える法制度面の対応，それぞれの連携が必要であろう.

本論文では,ビットコインシステムを対象に,P2PKHの資産移転方式に限定しているが，利用者であるトランザクション作成者の特定・追跡の仕組みの実現方式を複数提案し，その実現可能性，実現へのアプローチ案を示した．今回の実現方式案は，資産移転記録ベースの多くの暗号資産システム（TCAMS）へ適用可能と想定されるが，それぞれの暗号資産システムごとに別途検討が必要であろう.

暗号資産システムへの利用者の特定・追跡の仕組みの組み込みについての検討は，未だこれからの状況である．インターネット社会の安心・安全な暗号資産システム，さらには各国での検討が活発になってきたCBDC（法定デジタル通貨）の検討においても，利用者の匿名性と特定・追跡の両立が，重要な要件の一つであり，今後も多くの研究・開発が展開されることを期待したい.

謝辞　本研究の一部は，JSPS 科研費　基盤(B) JP18H03240 の支援を受けている.

文　献

[1] 才所敏明，辻井重男，櫻井幸一，“暗号資産の封印・償還における利用者の匿名性および特定・追跡性の考察”，暗号と情報セキュリティシンポジューム（SCIS2021）.

[2] 才所敏明，辻井重男，櫻井幸一，“暗号資産の匿名性要件の整理と対応レベルの比較”，コンピュータセキュリティシンポジューム（CSS2020）.

[3] 才所敏明，辻井重男，櫻井幸一，“暗号資産台帳の匿名性と特定・追跡性についての考察”，2020 年電子情報通信学会ソサイエティ大会.

[4] 才所敏明，辻井重男，“インターネット上のサービスにおける利用者の匿名性と特定・追跡性の両立”，暗号と情報セキュリティシンポジューム（SCIS2021）.

[5] 才所敏明，辻井重男，“インターネット時代の本人確認基盤に関する考察－ NAF から GAF へ－”，コンピュータセキュリティシンポジューム 2020（CSS2020）.

[6] CipherTrace Geographic Risk Report:VASP KYC by Jurisdiction，2020. https://ciphertrace.com/wp-content/uploads/2020/10/CipherTrace-2020-Geographic-Risk-Report-100120.pdf

[7] INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION（The FATF Recommendations），FATF，2020. https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/fatf%20recommendations%202012.pdf